Teknik uyarı: CL4/6NX Plus yazıcılarda güvenlik açığı keşfedildi

Eylül30, 2024

Özet

Bazı SATO etiket yazıcılarının, işlemleri etkileyebilecek yanlış/uygunsuz yetkilendirme (CWE-863, CWE-287) ve yol geçişi (CWE-22) ile ilgili güvenlik açıkları olduğu bulundu.

Bu güvenlik açıklarının istismar edildiğine dair bilinen bir durum yoktur ve yazıcı kullanıcıları, sistemlerini yetkisiz erişime karşı korumak için önlemler aldıkları sürece veri tahrifi veya bilgi ifşası riski altında değildir. Ancak, kullanıcılara, güvenliği artırmak için yazıcılarına aşağıdaki geçici çözümü uygulamalarını öneriyoruz.

Etkilenen yazıcılar

- CL4/6NX Plus
- CL4/6NX-J Plus (Japon Modeli)

Detaylar

Etkilenen yazıcılar, kullanıcıların web tarayıcısı üzerinden yazıcı ayarlarını görüntülemeleri veya değiştirmeleri için bir WebConfig işlevi sunar. Bu işlev, kullanıcı oturum açmayı gerektiren ve yanlış/uygunsuz yetkilendirmeye karşı savunmasız olabilen özellikler içerir (CWE-863, CWE-287). Bazı özellikler ayrıca saldırganların dosya sistemini dolaşmasına ve kısıtlanmış dizinlere erişmesine olanak tanıyan bir yol geçişi (CWE-22) güvenlik açığına sahiptir. Bu güvenlik açığı noktaları, yetkisiz ayar değişikliklerine ve dosya kurcalamasına yol açabilir ve yazıcıların çalışma şeklini etkileyebilir.

Çözüm

Güvenlik açıklarını kapatmak için yeni bir yazıcı aygıt yazılımı güncellemesi yayınlıyoruz. Aygıt yazılımını güncelleme hakkında bilgi için lütfen en yakın SATO temsilcinizle veya ürünü satın aldığınız dağıtımcıyla iletişime geçin. Lütfen randevu ayarlamak için bizimle iletişime geçin.

Geçici Çözüm

Kullanıcılar yazıcının güvenlik duvarını etkinleştirerek ve WebConfig işlevini devre dışı bırakarak güvenlik açıklarını aşabilirler. Ancak, bunun yalnızca belirli teknik nedenlerden dolayı aygıt yazılımı güncellemesini yükleyememeniz durumunda önerildiğini lütfen unutmayın.

- Çözüm yolunu uygulamak için aşağıdaki adımları izleyin. Daha fazla bilgi için çevrimiçi kullanıcı kılavuzumuzdaki "Ürünün Çeşitli Ayarları" bölümüne de bakabilirsiniz. (https://www.manual.sato-global.com/printer/cl4nx_cl6nx/main/toc.html)
  - Güvenlik duvarını etkinleştirin:
    Yazıcının Ayarlar menüsüne gidin ve Arayüz> Ağ> Gelişmiş> Güvenlik Duvarı> Etkinleştir'e tıklayın.
  - WebConfig'i devre dışı bırakın:
    Yazıcının Ayarlar menüsüne gidin ve Arayüz> Ağ> Gelişmiş> Güvenlik Duvarı> Hizmetlere ve Bağlantı Noktalarına İzin Ver> WebConfig> Devre Dışı Bırak'a tıklayın.

Sorularınız ve talepleriniz için lütfen buradaki iletişim formumuzu doldurun.

当社製ラベルプリンタ製品の脆弱性対応について

2024 年 8 月 30 日
株式会社サトー

概要

当社製ラベルプリンタの一部機種において、複数の脆弱性（不正な認証（CWE-863, CWE-287）、パス・トラバーサル（CWE-22））が発見されております。本脆弱性により当社製ラベルプリンタの動作に影響を与える可能性があります。

以下に示す対策または、回避策を実施することで、本脆弱性を無効化することが出来ます。

本脆弱性による被害は現時点では確認されておりません。お客様のシステムを経由した不正なアクセスがない限り、データの改ざんや情報漏洩の危険はありませんが、より安心して製品をお使いいただくため、本脆弱性への対応方法等を以下の通りご案内致します。

対象となる製品

当社製品で、本脆弱性に該当し、対策ファームウェアを準備している製品は下記製品となります。

- スキャントロニクス CL4/6NX-J Plus シリーズ
- スキャントロニクス CL4/6NX Plus シリーズ（海外向けモデル）

脆弱性内容

対象製品は、ウェブブラウザから設定確認・設定変更を可能とする WebConfig 機能を搭載しています。この WebConfig 機能の一部機能において認証が不十分（CWE-863, CWE-287）な脆弱性があります。また、WebConfig 機能の一部機能においてデータチェックが不十分（CWE-22）な脆弱性があります。これらの脆弱性により、意図しない設定変更やファイルの改ざんにより、対象製品の動作に影響を与える可能性があります。

対策方法

以下の対策により本脆弱性に対する対策が可能です。

- 対策ファームウェアを適用する。

当社製品の本体ファームウェア更新に関しては、お近くのサトー拠点もしくは商品を購入頂いた販売店へお問い合わせください。作業の依頼は、お問合せください。

回避方法

以下の対策により本脆弱性の回避が可能ですが、当社としましては、前述の対策ファームウェアの適用による対策を推奨します。何らかの理由により対策ファームウェアを適用できない場合は、本回避方法による対策をお願いします。

- ファイアウォール機能を有効にしたうえで、WebConfig 機能を無効とする。本対策では、対策ファームウェアの適用は不要です。ファイアウォール機能の有効化および、WebConfig 機能の無効化は、以下のオンラインマニュアルの記載を参照願います。
  - オンラインマニュアル： https://www.sato.co.jp/webmanual/printer/clnx-jplus/main/toc.html
    - ファイアウォール設定： 本製品の［設定］メニュー ＞ ［通信設定］メニュー ＞ ［ネットワーク］ ＞ ［詳細設定］ ＞ ［ファイアウォール］ ＞ ［有効］
    - WebConfig 設定： 本製品の［設定］メニュー ＞ ［通信設定］メニュー ＞ ［ネットワーク］ ＞ ［詳細設定］ ＞ ［ファイアウォール］ ＞［許可するサービス・ポート］ ＞ ［WebConfig］＞ ［無効］

本件に関するお問い合わせ先

本件に関するお問い合わせは、お客様ヘルプディスクにて承ります。

電話による問い合わせ： 0120-696310 （受付時間：24 時間 365 日）
お問い合わせフォーム： https://www.sato.co.jp/contact/support/